

**GUARDFORCE SECURITY LIMITED**

**Protection with Intelligence**

**[](https://www.sia.homeoffice.gov.uk/Pages/acs-roac.aspx)[](http://www.bsigroup.com/)**

SECURITY OPERATIONS MANAGEMENT POLICY

SUMMARY

**CONTENTS**

1. Policy Statement

2. Scope

3. Communication with Staff

4. Communications with Clients, Interested Parties

5. Surveys

6. Scope of Applicability

7. Principle of Conduct for SOMS

8.Strategic Programme

9. Supervision & Control

10. Document History

|  |  |  |
| --- | --- | --- |
| Date: | March 2024 | Objective –To ensure effective Security Operations management within the company, ensure compliance to ICoCA, ISO18788 and associated industry standards. |
| Issue: | 1 |
| Review Date: | March 2025 |
| Policy Number | GFS- POL - 032 |

|  |  |  |
| --- | --- | --- |
|  | Compiled | Approved |
|  | Robert Hanratty (Compliance Manager) | Warren Jones (Director) |



## **Policy Statement**

Top Management at GFS have the ability to design, assess and continuously revise the Security Operations Management (SOM) of the company and specifically to approve and update policies, which contain the guidelines governing the conduct of the company.

The purpose of this Policy is to establish the main principles of conduct that are to govern SOM within the company, to ensure the effective protection of people, of physical assets, of information as well as of privacy of processed data, at all times endeavouring to ensure that SOM activities are fully in accordance with the law and fully comply with the provisions of the company’s Human Rights Policy and additional noted commitments.

This document sets out GFS’s Policy in relation to all forms of security operations management with the public, press, partner organisations, contractors, consultants and staff.

The policy is designed to clarify and explain the basic rules for making the best use of GFS security operations management, it explains the company’s expectations and sets out general standards regarding security operations management.

Through this Policy, the Company states its commitment to excellence in terms of security services, understanding increased levels of demands from regulators, from customers and from the other stakeholders with which the company has a relationship.

1. **Scope**

This Policy applies to all staff at GFS and sets the standards the Company expects in relation to all forms of SOM.

Where supplier organisations carry out work or activities on behalf of GFS they may already have their own policies regarding SOM standards, however, GFS standards should be regarded as the minimum.

**Associated working:** Associated documents to implementation and maintaining the SOMS sits within the company’s HSEQ MS and is inclusive of all needs for effective working and management of the SOMS, and should be referenced to when confirming scope within the Policy.

1. **Communication with Staff (internal)**

The SOM Policy will be maintained and communicated to all company stakeholders through the Compliance element of the company in relationship with GFS Top Management, any changes to the Policy will be registered and all communications will be recorded within the company’s Communication Register.

1. **Communication with Clients, Subcontractors, Suppliers** **(interested parties)**

Communication regarding the SOM Policy to Clients and interested parties will be maintained as per point 3.

1. **Surveys**

Surveys for both staff and Clients are generated on a minimum bi-annual basis which are service element based and are presented and assessed at Management Review Meetings.

**6. Scope of Application**

This Policy applies all company staff at all levels.

This Policy is developed and supplemented by the following specific policies, also approved by the Top Management, that include but is not limited to;

- Human Rights Policy

- Data Protection Policy

- Risk Policy

- Diversity & Inclusivity Policy

- Whistle Blowing Policy

- Health & safety Policy

- Modern Slavery Policy

- Ethical Policy

**7. Main Principles of Conduct for SOM**

The following main principles of conduct that must drive the SOM activities of the company are:

a) Define a security strategy with a preventive and proactive approach to guarantee a reasonable level of risk.

b) Ensure the appropriate protection of assets, to proactively manage risks.

c) Ensure as far as is practical the protection of all staff, subcontractors, Clients and interested parties, as well as the protection of persons when in care under contract.

d) Define a security management model with a clear allocation of roles and responsibilities and effective coordination mechanisms, which integrates security and proactive risk management into decision-making processes.

e) Ensure the adequate protection of information and knowledge, to proactively manage risks to the provisions within the Cybersecurity Risk Policy.

f) Adopt the measures necessary to prevent, neutralise, minimise or restore the harm caused by physical, cybersecurity or hybrid security threats to normal business operations.

g) Encourage an inclusive culture and awareness regarding SOM within the company, through information dissemination, awareness-raising and training activities.

h) Promote appropriate security training for all staff, both internal and external.

i) Promote best practices and innovation in the area of SOM.

j) Collaborate with relevant Stakeholders (including the supply chain and customers) on security risks that affect the company and relationship, adding strength to a potential coordinated response to highlighted security risks and threats.

k) Provide all assistance and cooperation that may be requested by, including but not limited to, regulators, national forces and governmental agencies.

l) Always acting in accordance with applicable law and the provisions of the Code of Ethics.

**8. Strategic Security Programme**

In partnership with Top Management the Compliance and Operational leads shall identify, implement and evaluate the actions necessary to prepare a SOMS in accordance with the principles and guidelines defined in this Policy, and it shall develop the internal rules, methodologies and procedures to ensure the appropriate implementation of the SOM within the company.

The company maintains and reviews all business elements at monthly Management Reviews and is inclusive of business planning.

**9. Supervision and Control**

Top Management own this policy which is managed through the company’s Compliance Element and implemented through Operations, Administration, HR and Finance.

Regular evaluations and audits shall be performed with internal or external auditors in order to verify compliance with this Policy.

## **Owner: Top Management**

## **Change Management: Compliance**

## **Implementation: All departments**

## **Applicable to: All staff**

ISO18788 (5.3) Compliance requirement confirmations:

* Ensuring that the SOMS conforms to the requirements of this International Standard – *Compliance though ISO Standard management including audit.*
* Reporting on the performance of the SOMS to Top Management – *Compliance at monthly Management Reviews.*

- Ensuring that an SOMS is established, communicated, implemented and maintained

in accordance with the requirements of this International Standard – *Compliance*

*through SOM build, documented maintenance and with all stakeholders and*

*interested parties communicated with and recorded on a communications register.*

- Identifying, monitoring and managing the needs and expectations of stakeholders

set out in 4.2 – *Compliance through management of business risk elements recorded*

*within the company risk register.*

- Ensuring that adequate resources are made available – *Top Management through*

*Management Reviews and budget meetings.*

- Promoting awareness of SOMS requirements throughout the organization - *All*

*Departments through using and working with SOMS, ensuring compliance to working*

*polices and ensuring all staff are aware of requirements.*

- Reporting on the performance of the SOMS to top managers for review and as a

basis for continuous improvement *– Top Management and Compliance at regular*

*recorded meetings and submission of KPI documents both internal and external.*

- Top Management shall ensure that those responsible for implementing and

maintaining the SOMS have the necessary authority and competence to do so and

are held accountable for its operation – *Authority levels are understood within the*

*company, line managers are defined within job descriptions, with Top management*

*having final say on decisions.*

It should be noted that the company hold working documents to cover all elements of SOMS management.

1. **Document History**

|  |  |  |  |
| --- | --- | --- | --- |
| March 2024 | Issue 1 | | Initial Document |
|  |  | |  |
|  | |  |  |
|  | |  |  |
|  | |  |  |